AF
JEW

Docket No.: **P-0303** PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	Confirmation No.: **3711**
Won Uk YU	Group Art Unit: **2152**
Serial No.: **09/996,718**	Examiner: **To Be Assigned**
Filed: **November 30, 2001**	Customer No.: **34610**

For: **METHOD FOR ACCESSING INTERNET USING INTERNET TV**

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

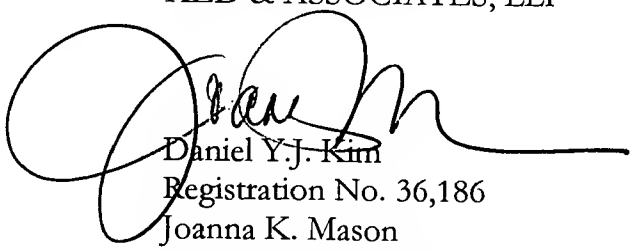
Sir:

In response to the Notification of Non-Compliant Appeal Brief dated May 7, 2007, the Status of the Claims section previously submitted in the March 20, 2007 Appeal Brief is amended to include a status of claim 17 (canceled), as requested in the Notice. Further, the Summary of the Claimed Subject Matter section is amended to include a mapping of all of independent claims 1, 2 and 7 to the corresponding section of the specification and figures, in addition to the element numbers previously included, as requested in the Notice. The Appeal Brief is also amended to include an Evidence Appendix submitting a copy of the Provisional Application Serial No. 60/186,551, a copy of which was attached to the Appeal Brief as originally filed. The Amended Appeal Brief is attached.

Should the Examiner have any questions regarding the above-identified application, the Examiner is invited to contact the undersigned at the telephone number listed below.

Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
KED & ASSOCIATES, LLP



Daniel Y.J. Kim
Registration No. 36,186
Joanna K. Mason
Registration No. 56,408

P. O. Box 221200
Chantilly, VA 20153-1200
703 766-3777
Date: **May 22, 2007**
Please direct all correspondence to Customer Number 34610
124983

Docket No.: P-0303 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCE

In re Application of	Confirmation No.: 3711
Won Uk YU	Group Art Unit: 2152
Serial No.: 09/996,718	Examiner: Changkong, Dohm
Filed: November 30, 2001	Customer No.: 34610

For: METHOD FOR ACCESSING INTERNET USING INTERNET TV

AMENDED APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief-Patents
Randolph Building
401 Dulany Street
Alexandria, Virginia 223134

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed November 21, 2006. This appeal is taken from the rejection of claims as set forth in the Office Action of August 22, 2006 (hereinafter the Office Action). In accordance with 37 C.F.R. §41.37, Applicant addresses the following items.

REAL PARTY IN INTEREST

The real party in interest is the assignee, LG ELECTRONICS INC. The assignment document is recorded at Reel 012340 and Frame 0137.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and interferences.

STATUS OF THE CLAIMS

This is an appeal from the final rejection dated August 22, 2006 of claims 1-16 and 18-24. Claims 1-16 and 18-24 are pending. Claim 17 was canceled in an Amendment filed on December 28, 2005. No other claims are pending.

STATUS OF AMENDMENTS

All Amendments filed in this application have been entered. A copy of appealed claims 1-16 and 18-24 appears in the attached Claims Appendix.

SUMMARY OF THE CLAIMED SUBJECT MATTER

As stated in 37 C.F.R §41.37(c)(v), Applicant is providing the following explanation of each of the independent claims 1, 2 and 7 involved in this appeal. This explanation refers to the specification and drawings. The following is merely an example summary and is not intended to be a discussion of the full and entire scope of the claims. Other interpretations, configurations and embodiments are also within the scope of the pending claims.

This relates to a system and method for accessing the Internet using an Internet TV in which an authentication number may be automatically provided to the Internet TV by a portal

server. This system and method allows for automatic access to information on the server, without repeated logins each time access is requested.

More specifically, to gain Internet access, an Internet enabled TV transmits an access request to a portal server, and the portal server requests an authentication number prior to providing access. If the authentication number is already stored in the TV's memory, the TV simply transmits the authentication number to the server, the server checks the number, and provides access to the server if the number checks correctly. If the authentication number is not stored in the TV's memory, then the TV requests that the server either search for its authentication number, or provide a new authentication number. Once the new authentication number is provided, access is granted, and the new number is stored in the TV for use during later sessions.

Independent Claim 1

Independent claim 1 is drawn to a method for accessing the Internet using an Internet TV in an Internet TV system comprising the Internet TV, in which a function of accessing the Internet and a function of receiving a TV broadcast are combined, and a server for operating a portal site which provides information to the Internet TV. Independent claim 1 recites transmitting a message from the Internet TV to the server requesting authentication for use of information during a current session [Fig. 4 (S310), Fig. 5 (S402, S403), page 5/lines 21-22, page 6/lines 20-22 and page 7/lines 8-16 of the specification]; transmitting a message from the server

requesting an authentication number from the Internet TV [Fig. 4 (S320), Fig. 5 (S404), page 5/lines 22-25 and page 7/lines 17-19 of the specification]; transmitting the requested authentication number from the Internet TV to the server if the authentication number is available [Fig. 4 (S330), Fig. 5 (S411), page 6/lines 4-7 and page 8/lines 2-5 of the specification], checking a validity of the transmitted authentication number [Fig. 5 (S412) and page 8, lines 5-7 of the specification], and providing information to the Internet TV for the current session if it is determined that the authentication number is valid [Fig. 4 (S340), Fig. 5 (S414), page 6/lines 7-10 and page 8/lines 7-11 of the specification]; requesting a new authentication number from the server if the authentication number is not available [Fig. 5 (S415) and page 9/lines 6-11 of the specification], registering a user in accordance with information collected by the server [Fig. 5 (S416) and page 9/lines 12-14 of the specification], receiving a new authentication number from the server [Fig. 5 (S417) and page 9/lines 14-16 of the specification], and providing information to the Internet TV for use during the current session [Fig. 5 (S414) and page 8/lines 7-11 of the specification]; and storing the new authentication number in a memory device of the Internet TV for use during a later session [Fig. 5 (S418) and page 9/lines 16-18 of the specification].

Independent Claim 2

Independent claim 2 is drawn to a method for accessing the Internet using an Internet TV. Independent claim 2 recites (a) transmitting a message requesting authentication for use of information to a portal server and transmitting a response from the portal server requesting transmission of an authentication number when the Internet TV is turned on [Fig. 4 (S310,

S320), Fig. 5 (S402, S403), page 5/lines 21-25, page 6/lines 20-22 and page 7/lines 8-16 of the specification]; (b) determining if the authentication number requested by the portal server is available [Fig. 5 (S410) and page 7/lines 24 – page 8/line 2 of the specification] and transmitting the authentication number to the portal server if the requested authentication number is already available [Fig. 4 (S330), Fig. 5 (S411), page 6/lines 4-7 and page 8/lines 2-5 of the specification], and determining an authentication number based on additional information collected by the portal server and transmitting the authentication number to the Internet TV for storage if the authentication number is not already available [Fig. 5 (S406, S407, S408, S409) and page 8/lines 14-24 of the specification]; and (c) transmitting information related to the message requesting authentication for use of information from the portal server to the Internet TV [Fig. 4 (S340), Fig. 5 (S414), page 6/lines 7-10 and page 8/lines 7-11 of the specification].

Independent Claim 7

Independent claim 7 is drawn to a method for accessing the Internet using an Internet TV. Independent claim 7 recites (a) requesting a portal server to obtain an authentication number when the portal server receives an access request message from an Internet TV with respect to the use of information [Fig. 5 (S406, S415), page 8/lines 17-21 and page 9/lines 6-11 of the specification]; (b) transmitting a new authentication number from the portal server to the Internet TV if the authentication number is not provided by the Internet TV [Fig. 5 (S408, S417), page 8/lines 21-24 and page 9/lines 12-18 of the specification], wherein the new authentication number is established based on additional information collected by the portal

server after the portal server receives the access request message if the authentication number is not provided by the Internet TV [Fig. 5 (S407, S416), page 8/lines 21-24 and page 9/lines 12-18 of the specification]; and (c) providing information related to the access request message with respect to the use of information to the Internet TV in response to the received access request message [Fig. 5 (S414) and page 8/lines 7-11 of the specification].

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Whether claims 1-16 and 18-24 are obvious under 35 U.S.C. §103(a) over Figures 1-3 of the present application in view of U.S. Patent No. 6,785,716 to Nobakht, and further in view of U.S. Patent Publication No. 2003/0095791 to Barton et al. (hereinafter "Barton").

In the section below entitled "Arguments," Applicant sets forth separate arguments for each of pending claims 1-16 and 18-24. Applicant respectfully submits that each of claims 1-16 and 18-24 stands and falls separately from one another.

ARGUMENTS

The present application includes three independent claims, namely, independent claims 1, 2 and 7. These claims recite different features as may be evidenced by the discussion below. However, for ease of discussion, in some instances, similar features may be discussed with respect to one another. This is not an admission that the claims are the same, or that they stand or fall together. Rather, this is an attempt to narrow the number of issues and limit the number of arguments. While arguments may be similar for different claims, it should be understood that differently claimed features are expressly recited in different claims.

It is respectfully submitted that each of the independent claims defines patentable subject matter, as discussed below. Each of the dependent claims depends from one of the independent claims, and therefore defines patentable subject matter at least for this additional reason.

Further, each of the dependent claims recite features that further and independently distinguish over the applied prior art.

I. Rejection Under 35 U.S.C. §103(a) over Figures 1-3 of the Present Application in view of Nobakht and Barton

It is noted that the present application was filed on November 30, 2001, claiming priority to Korean Patent Application 72949/2000 filed in Korea on December 4, 2000. A Certified Translation of the corresponding Korean Priority Document was filed on June 22, 2006 to perfect the claim for priority. The December 4, 2000 priority date of the present application clearly predates Barton's February 27, 2001 PCT filing date. Accordingly, only the subject matter supported by U.S. Provisional Application No. 60/186,551 filed March 2, 2000 (hereinafter "the Barton provisional application") may be relied upon in rejection of the claims of the present application. A copy of the Barton provisional application is provided herewith.

A. Independent Claim 1

Independent claim 1 is drawn to a method for accessing the Internet using an Internet TV in an Internet TV system comprising the Internet TV, in which a function of accessing the Internet and a function of receiving a TV broadcast are combined, and a server for operating a portal site which provides information to the Internet TV. Independent claim 1 recites transmitting a message from the Internet TV to the server requesting authentication for use of

information during a current session, transmitting a message from the server requesting an authentication number from the Internet TV, and transmitting the requested authentication number from the Internet TV to the server if the authentication number is available, checking a validity of the transmitted authentication number, and providing information to the Internet TV for the current session if it is determined that the authentication number is valid. Independent claim 1 also recites requesting a new authentication number from the server if the authentication number is not available, registering a user in accordance with information collected by the server, receiving a new authentication number from the server, providing information to the Internet TV for use during the current session, and storing the new authentication number in a memory device of the Internet TV for use during a later session.

As acknowledged in the Office Action in the remarks regarding independent claim 1, Figures 1-3 of the present application neither disclose nor suggest each of the features recited in independent claim 1, or the claimed combination of features, and Nobakht alone fails to over come the deficiencies of Figures 1-3 of the present application. Further, Barton, and in particular, the subject matter supported by the Barton provisional application, fails to overcome the deficiencies of Figures 1-3 of the present application and Nobakht.

Nobakht discloses a channel based Internet network 100, including a system server 110, Internet sites 120, and user terminals 130, user terminal 130A including a display 132 connected to a separate set top box 131 controlled by an input device 133. As shown in Figure 3A of Nobakht, in response to a user login, user request, and authorization by the server, the system

displays channel tables 219 on the display 132 which provide website links to channels previously selected by a user.

As shown in Figure 7 of Nobakht, in order to gain access to service when the set top box 131 detects the presence of a smart card (step705), the set top box 131 transmits a service request message to the server 110 (step 715), and the server 100 responds with a request for login information (step 720). The set top box 131 accesses relevant account information and transmits it to the server (step 725), which checks the account information for validity (step 730). If the account is not valid, a customer service page is transmitted to the set top box 131 (step 760) and displayed on the display 132 (step 765). If the account is valid and the server determines that the user is an authorized resident user based on information from the smart card, then access is granted (step 745-1), allowing the resident user to store and manipulate a channel table (steps 800 and 900).

If the account is valid but the user is not a resident user (based on information in the smart card), the server 110 transmits a message to the set top box 131 asking the set top box 131 if the guest user is allowed (step 740). The set top box 131 then checks for flags set by the owner of the set top box 131 which indicate whether or not access is allowed for the guest user (step 750). If the guest user is not allowed, the customer service page is displayed (step 765). If the guest user is allowed, then the server 110 grants access to the guest user, allowing the guest user to store and manipulate a channel table (steps 800 and 900).

Thus, in the event that a guest user is requesting access, the server 110 simply transmits a message to the set top box 131 asking if this access is allowed, and the set top box provides approval or denial of the guest's access request. However, the access provided to the guest user simply allows for use during the current session. Nobakht neither discloses nor suggests that this includes any type of transmission and/or storage of an authentication number, let alone a new authentication number, either by the server 110 or the set top box 131, which could be used for immediate access during a later session, and without first proceeding through the entire login process once again in order to gain access. Further, when the necessary information cannot be provided, the user is simply sent to a customer service page, and Nobakht neither discloses nor suggests that, in any of the situations discussed above, the server transmits an authentication number, let alone a new authentication number, to the set top box 131 and/or display 132 when the necessary information cannot be provided by the user terminal 130.

Nobakht neither discloses nor suggests requesting a new authentication number from the server if the authentication number is not available, registering a user in accordance with information collected by the server, receiving a new authentication number from the server, providing information to the Internet TV for use during the current session, and storing the new authentication number in a memory device of the Internet TV for use during a later session, as recited in independent claim 1.

Still further, Nobakht's system relies on the capability of a separate set top box 131 to provide access to the information provided by the server for display on the display device 132.

Nobakht neither discloses nor suggests a using an Internet TV, in which a function of accessing the Internet and a function of receiving a TV broadcast are combined, nor that the capabilities of the network 100 disclosed by Nobakht could or should be incorporated into an Internet TV.

The Barton provisional application discloses a system for using MPEG for digital audio and video transmission. In this system, MPEG streams and accompanying events tables may be encrypted, preferably separately, prior to transmission to prevent unauthorized use. By encrypting the MPEG stream and event tables separately, the events tables may be decrypted on the receiving end without decrypting the entire MPEG stream, thus simplifying the decryption process. TiVo receivers may be used to distribute these audio/video streams to a large population. An owner of one of the TiVo receivers may access the audio/video streams once proper authorization for decryption is provided.

The Office Action asserts that the Barton provisional application teaches on pages 12-15 the use of encryption keys that are exchanged over a network. However, page 12 merely discloses that pre-encrypted media streams are locally decrypted, and only when they are viewed, thereby protecting the content from theft when not in use. For example, if the media stream is transferred from a first receiver to a second receiver, and then viewed only by a viewer of the second receiver, only the viewer of the second receiver is appropriately charged in line with established copy protection rules. Pages 13 and 14 further disclose how additional interaction between receivers may be enabled, but make no mention of the use of encryption/decryption/authentication keys or numbers to do so.

The Office Action further asserts that the Barton provisional application teaches on page 6 the distribution of authentication keys. However, pages 6 and 7 of the Barton provisional application merely set forth process steps for pairing, recording and playback procedures, and associated keys which may be used with each. The Barton provisional application neither discloses nor suggests that at any point in any of these procedures, the validity of any of the keys is checked, either before, during or after transmission from one receiver to another, and thus necessarily neither discloses nor suggests that at any point, during any of these procedures, a new key may be requested and/or transmitted if an existing key is determined to be invalid, nor that such a newly requested key is stored for use during a later session. Thus, the Barton provisional application neither discloses nor suggests requesting a new authentication number from the server if an authentication number is not available, registering a user in accordance with information collected by the server, receiving a new authentication number from the server, providing information to the Internet TV for use during the current session, and storing the new authentication number in a memory device of the Internet TV for use during a later session, as recited in independent claim 1.

Applicant respectfully disagrees with the assertion in the Office Action that the mere disclosure of encryption and decryption keys in the Barton provisional application provides adequate support for applying, in a rejection of the present application, the use of cookies allegedly disclosed in the later Barton publication. More specifically, Applicant respectfully submits that the use of these keys in Barton provisional application is limited to encryption and

decryption. The mere identification of these keys does not necessarily render obvious or evident their eventual use, and particularly the exchange, authentication, provision and storage of these keys, nor does it provide support for the manner in which the keys are used as specifically set forth in the Barton publication, contrary to what is asserted in the Office Action. Thus, Applicant respectfully submits that Barton is entitled to the earlier filing date of the provisional application only for the subject matter which is supported by the provisional application, and that the subject matter relied in the rejection set forth in the Office Action is not supported by the Barton provisional application.

For at least these reasons, it is respectfully submitted that independent claim 1 is allowable over the applied combination, and thus the rejection of independent claim 1 under 35 U.S.C. §103(a) over Figures 1-3 of the present application, Nobakht and Barton should be withdrawn.

B. Dependent Claim 18

Dependent claim 18 depends from independent claim 1, and therefore is allowable at least for this reason. However, dependent claim 18 recites additional features such that dependent claim 18 does not stand or fall together with independent claim 1. For example, dependent claim 18 recites that checking a validity of the transmitted authentication number comprises checking for an error in the authentication number, accessing user information in a database if an error is not detected in the authentication number, and providing information to the Internet TV regarding user fees if the user information indicates that a user is registered.

However, as acknowledged in the Office Action issued on March 27, 2006, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of claim 18. The Office Action asserts Office Notice of the alleged obviousness of this feature, but provides no prior art reference to establish such obviousness. Accordingly, it is respectfully submitted than the applied prior art references provide no teaching or suggestion for the features of claim 18, let alone in combination with the other features of independent claim 1. Thus, dependent claim 18 is allowable at least for this additional reason.

C. Dependent Claim 19

Dependent claim 19 depends from dependent claim 18 which depends from independent claim 1, and therefore is allowable at least for this reason. However, dependent claim 19 recites additional features such that dependent claim 19 does not stand or fall together with dependent claim 18 or independent claim 1. For example, dependent claim 19 recites transmitting an error message when an error is detected in the authentication number, requesting user information from the Internet TV and determining whether the user is registered in the database, and transmitting a corrected authentication number if the user is registered in the database. However, as set forth above, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of claim 19, let alone in combination with the other features of independent claim 1

and/or dependent claim 18. Thus, dependent claim 19 is allowable at least for this additional reason.

D. Dependent Claim 20

Dependent claim 20 depends from independent claim 1, and therefore is allowable at least for this reason. However, dependent claim 20 recites additional features such that dependent claim 20 does not stand or fall together with independent claim 1. For example, dependent claim 20 recites determining if the Internet TV is in a default state. However, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion that any of the respective systems disclosed therein enter a default state. Thus, the applied prior art references provide no teaching or suggestion for the features of claim 20, let alone in combination with the other features of independent claim 1. Thus, dependent claim 20 is allowable at least for this additional reason.

E. Dependent Claim 21

Dependent claim 21 depends from independent claim 1, and therefore is allowable at least for this reason. However, dependent claim 21 recites additional features such that dependent claim 21 does not stand or fall together with independent claim 1. For example, dependent claim 21 recites storing the new authentication number in a memory device of the Internet TV. However, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion

for the features of claim 21, let alone in combination with the other features of independent claim 1. Thus, dependent claim 21 is allowable at least for this additional reason.

F. Independent Claim 2

Independent claim 2 is directed to a method for accessing the Internet using an Internet TV. Independent claim 2 recites (a) transmitting a message requesting authentication for use of information to a portal server and transmitting a response from the portal server requesting transmission of an authentication number when the Internet TV is turned on, and (b) determining if the authentication number requested by the portal server is available and transmitting the authentication number to the portal server if the requested authentication number is already available, and determining an authentication number based on additional information collected by the portal server and transmitting the authentication number to the Internet TV for storage if the authentication number is not already available. Independent claim 2 also recites (c) transmitting information related to the message requesting authentication for use of information from the portal server to the Internet TV.

As acknowledged by the Examiner in the remarks regarding independent claim 2, Figures 1-3 of the present application neither disclose nor suggest each of the features recited in independent claim 2, or the claimed combination of features, and Nobakht alone fails to over come the deficiencies of Figures 1-3 of the present application. Further, as set forth above, Barton, and in particular, the Barton provisional application, fails to overcome the deficiencies of Figures 1-3 of the present application and Nobakht.

More specifically, as set forth above, the Barton provisional application discloses that pre-encrypted media streams are decrypted only when they are viewed, and that only the viewer is charged for the viewed media stream, even when additional interaction between receivers is enabled. However, the Barton provisional application is silent as to the use of encryption/decryption/authentication numbers to do so. Further, the Barton provisional application neither discloses nor suggests that at any point such authentication keys or numbers are valid or available, either before, during or after transmission from one receiver to another. Thus, the Barton provisional application neither discloses nor suggests that additional information may be collected and such an authentication key or number may be requested and/or transmitted, nor that this authentication key or number may be stored for use during a later session, as recited in independent claim 2. Thus, the Barton provisional application fails to overcome the deficiencies of Figures 1-3 of the present application and Nobakht.

For at least these reasons, it is respectfully submitted that independent claim 2 is allowable over the applied combination, and thus the rejection of independent claim 2 under 35 U.S.C. §103(a) over Figures 1-3 of the present application, Nobakht and Barton should be withdrawn.

G. Dependent Claim 3

Dependent claim 3 depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 3 recites additional features such that dependent claim 3 does not stand or fall together with independent claim 2. For example, dependent claim

3 recites that the if the Internet TV is in a default state, requesting the portal server to search for an authentication number corresponding to the Internet TV when the Internet TV is in a default state, inputting user information requested by the portal server, and receiving the requested authentication number and storing the received authentication number in a memory device. However, as set forth above, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 3, let alone in combination with the features of independent claim 2. Thus, dependent claim 3 is allowable at least for this additional reason.

H. Dependent Claim 4

Dependent claim 4 depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 4 recites additional features such that dependent claim 4 does not stand or fall together with independent claim 2. For example, dependent claim 4 recites that if the authentication number is not available, requesting the portal server to provide a new authentication number with respect to the use of information, and receiving a new authentication number from the portal server and storing the authentication number in a memory device. However, as set forth above, Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 4, let alone in combination with the features of independent claim 2. Thus, dependent claim 4 is allowable at least for this additional reason.

I. Dependent Claim 5

Dependent claim 5 depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 5 recites additional features such that dependent claim 5 does not stand or fall together with independent claim 2. For example, dependent claim 5 recites that step (c) above comprises (c1) examining the authentication number, and (c2) receiving information from the portal server when it is determined from the examination of the authentication number that the authentication number is a normal authentication number. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 5, let alone in combination with the features of independent claim 2. Thus, dependent claim 5 is allowable at least for this additional reason.

J. Dependent Claim 6

Dependent claim 6 depends from dependent claim 5 which depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 6 recites additional features such that dependent claim 6 does not stand or fall together with dependent claim 5 or independent claim 2. For example, dependent claim 6 recites providing user information requested by the portal server when it is determined from the examination of the authentication number that the authentication number is not a normal authentication number, and receiving an authentication number transmitted from the portal server and storing the received authentication number in a memory device. Figures 1-3 of the present application

and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 6, let alone in combination with the features of independent claim 2 and/or dependent claim 5. Thus, dependent claim 6 is allowable at least for this additional reason.

K. Dependent Claim 22

Dependent claim 22 depends from dependent claim 4 which depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 22 recites additional features such that dependent claim 22 does not stand or fall together with dependent claim 4 or independent claim 2. For example, dependent claim 22 recites registering a user in accordance with a user registration form requested by the portal server. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 22, let alone in combination with the features of independent claim 2 and/or dependent claim 4. Thus, dependent claim 2 is allowable at least for this additional reason.

L. Dependent Claim 24

Dependent claim 24 depends from dependent claim 3 which depends from independent claim 2, and therefore is allowable at least for this reason. However, dependent claim 24 recites additional features such that dependent claim 24 does not stand or fall together with dependent claim 3 or independent claim 2. For example, dependent claim 24 recites accessing the stored authentication number to gain access to the Internet during a later session. Figures 1-3 of the

present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 24, let alone in combination with the features of independent claim 2 and/or dependent claim 3. Thus, dependent claim 22 is allowable at least for this additional reason.

M. Independent Claim 7

Independent claim 7 is directed to a method for accessing the Internet using an Internet TV. Independent claim 7 recites (a) requesting a portal server to obtain an authentication number when the portal server receives an access request message from an Internet TV with respect to the use of information, and (b) transmitting a new authentication number from the portal server to the Internet TV if the authentication number is not provided by the Internet TV, wherein the new authentication number is established based on additional information collected by the portal server after the portal server receives the access request message if the authentication number is not provided by the Internet TV. Independent claim 7 also recites (c) providing information related to the access request message with respect to the use of information to the Internet TV in response to the received access request message.

As acknowledged in the Office Action in the remarks regarding independent claim 7, and as set forth above, Figures 1-3 of the present application neither disclose nor suggest each of the features recited in independent claim 7, or the claimed combination of features, and Nobakht alone fails to over come the deficiencies of Figures 1-3 of the present application. Further, as set

forth above, Barton, and in particular, the Barton provisional application, fails to overcome the deficiencies of Figures 1-3 of the present application and Nobakht.

More specifically, as set forth above, the Barton provisional application is silent as to the use of encryption/decryption/authentication numbers to decrypt pre-encrypted media streams for viewing. Further, the Barton provisional application neither discloses nor suggests that at any point new or additional information may be collected so that a new authentication key or number may be transmitted, as recited in independent claim 7. Thus, the Barton provisional application fails to overcome the deficiencies of Figures 1-3 of the present application and Nobakht.

For at least these reasons, it is respectfully submitted that independent claim 7 is allowable over the applied combination, and thus the rejection of independent claim 7 under 35 U.S.C. §103(a) over Figures 1-3 of the present application, Nobakht and Barton should be withdrawn.

N. Dependent Claim 8

Dependent claim 8 depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 8 recites additional features such that dependent claim 8 does not stand or fall together with independent claim 7. For example, dependent claim 8 recites the portal server remains in a stand-by state waiting for an access request message. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of

dependent claim 8, let alone in combination with the features of independent claim 7. Thus, dependent claim 2 is allowable at least for this additional reason.

O. Dependent Claim 9

Dependent claim 9 depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 9 recites additional features such that dependent claim 9 does not stand or fall together with independent claim 7. For example, dependent claim 9 recites requesting the Internet TV to provide user information when the received access request message requests the portal server to search for an authentication number; and determining whether a user is registered in a database when the user information is received and transmitting an authentication number if the user is registered. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 9, let alone in combination with the features of independent claim 7. Thus, dependent claim 9 is allowable at least for this additional reason.

P. Dependent Claim 10

Dependent claim 10 depends from dependent claim 9 which depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 10 recites additional features such that dependent claim 10 does not stand or fall together with dependent claim 9 or independent claim 7. For example, dependent claim 10 recites requesting the Internet TV to provide user information when it is determined that a user is not registered in the

database; and assigning a new authentication number to the Internet TV when the user information is received and transmitting the assigned authentication number to the Internet TV. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 10, let alone in combination with the features of independent claim 7 and/or dependent claim 9. Thus, dependent claim 10 is allowable at least for this additional reason.

Q. Dependent Claim 11

Dependent claim 11 depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 11 recites additional features such that dependent claim 11 does not stand or fall together with independent claim 7. For example, dependent claim 11 recites checking for an error in the authentication number when the received access request message includes an authentication number; determining whether the user is registered in a database when an error is not detected in the authentication number; and providing information to the Internet TV according to whether a user fee is paid when it is determined that the user is registered in the database. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 11, let alone in combination with the features of independent claim 7. Thus, dependent claim 11 is allowable at least for this additional reason.

R. Dependent Claim 12

Dependent claim 12 depends from dependent claim 10 which depends from dependent claim 9 which depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 12 recites additional features such that dependent claim 12 does not stand or fall together with dependent claim 10, dependent claim 9 or independent claim 7. For example, dependent claim 12 recites that the error is checked using a check sum method. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 12, let alone in combination with the features of independent claim 7 and/or dependent claim 10. Thus, dependent claim 12 is allowable at least for this additional reason.

S. Dependent Claim 13

Dependent claim 13 depends from dependent claim 10 which depends from dependent claim 9 which depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 13 recites additional features such that dependent claim 13 does not stand or fall together with dependent claim 10, dependent claim 9 or independent claim 7. For example, dependent claim 13 recites transmitting an error message when an error is detected in the authentication number; requesting the Internet TV to provide user information and determining whether the user is registered in the database; and transmitting a corresponding authentication number when it is determined that the user is registered in the database. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either

alone or in combination, provide no teaching or suggestion for the features of dependent claim 13, let alone in combination with the features of independent claim 7 and/or dependent claims 9 and/or 10. Thus, dependent claim 13 is allowable at least for this additional reason.

T. Dependent Claim 14

Dependent claim 14 depends from dependent claim 10 which depends from dependent claim 9 which depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 14 recites additional features such that dependent claim 14 does not stand or fall together with dependent claim 10, dependent claim 9 or independent claim 7. For example, dependent claim 14 recites registering the user in the database and providing information to the Internet TV when the user information is received. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 14, let alone in combination with the features of independent claim 7 and/or dependent claims 9 and/or 10. Thus, dependent claim 14 is allowable at least for this additional reason.

U. Dependent Claim 15

Dependent claim 15 depends from dependent claim 10 which depends from dependent claim 9 which depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 15 recites additional features such that dependent claim 15 does not stand or fall together with dependent claim 10, dependent claim 9 or independent claim 7. For example, dependent claim 15 recites determining whether a user fee is paid; and

transmitting a message to the Internet TV informing that the user fee is not paid if it is determined that the user fee is not paid. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 15, let alone in combination with the features of independent claim 7 and/or dependent claims 9 and/or 10. Thus, dependent claim 15 is allowable at least for this additional reason.

V. Dependent Claim 16

Dependent claim 16 depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 16 recites additional features such that dependent claim 16 does not stand or fall together with independent claim 7. For example, dependent claim 16 recites requesting the Internet TV to provide the user information when the received access request message requests the portal server to provide a new authentication number; and registering the user, assigning a new authentication number to the Internet TV, and transmitting the new authentication number when the user information is received. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 16, let alone in combination with the features of independent claim 7. Thus, dependent claim 16 is allowable at least for this additional reason.

W. Dependent Claim 23

Dependent claim 23 depends from independent claim 7, and therefore is allowable at least for this reason. However, dependent claim 23 recites additional features such that dependent claim 23 does not stand or fall together with independent claim 7. For example, dependent claim 23 recites that the authentication number is accessed from a memory device of the Internet TV if the authentication number is provided by the Internet TV. Figures 1-3 of the present application and/or Nobakht and/or the Barton provisional application, either alone or in combination, provide no teaching or suggestion for the features of dependent claim 23, let alone in combination with the features of independent claim 7. Thus, dependent claim 23 is allowable at least for this additional reason.

CLAIMS APPENDIX

The attached Claims Appendix contains a copy of the claims involved in the appeal.

EVIDENCE APPENDIX

The Attached Evidence Appendix includes a copy of Provisional Application Serial No. 60/186,551 filed on March 20, 2000 by Barton et al.

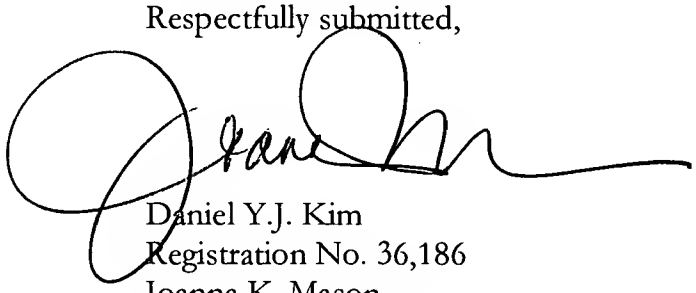
RELATED PROCEEDINGS APPENDIX

Applicant is not providing copies of related decisions and therefore a Related Proceeding Appendix is not provided.

CONCLUSION

It is respectfully submitted that the above arguments show that each of claims 1-16 and 18-24 are patentable over the applied references. Based at least on these reasons, it is respectfully submitted that each of claims 1-16 and 18-24 defines patentable subject matter. Applicant respectfully requests that the rejections of claims 1-16 and 18-24 set forth in the August 22, 2006 Office Action be withdrawn.

Respectfully submitted,



Daniel Y.J. Kim
Registration No. 36,186
Joanna K. Mason
Registration No. 56,408

Attachment:
Barton Provisional Application

P. O. Box 221200
Chantilly, Virginia 20153-1200
703 766-3777 DYK/JKM/lhd
Date: May 22, 2007
Please direct all correspondence to Customer Number 34610
124984

CLAIMS APPENDIX

1. A method for accessing the Internet using an Internet TV in an Internet TV system comprising the Internet TV, in which a function of accessing the Internet and a function of receiving a TV broadcast are combined, and a server for operating a portal site which provides information to the Internet TV, the method comprising:

transmitting a message from the Internet TV to the server requesting authentication for use of information during a current session;

transmitting a message from the server requesting an authentication number from the Internet TV;

transmitting the requested authentication number from the Internet TV to the server if the authentication number is available, checking a validity of the transmitted authentication number, and providing information to the Internet TV for the current session if it is determined that the authentication number is valid;

requesting a new authentication number from the server if the authentication number is not available, registering a user in accordance with information collected by the server, receiving a new authentication number from the server, and providing information to the Internet TV for use during the current session; and

storing the new authentication number in a memory device of the Internet TV for use during a later session.

2. A method for accessing the Internet using an Internet TV, comprising:

(a) transmitting a message requesting authentication for use of information to a portal server and transmitting a response from the portal server requesting transmission of an authentication number when the Internet TV is turned on;

(b) determining if the authentication number requested by the portal server is available and transmitting the authentication number to the portal server if the requested authentication number is already available, and determining an authentication number based on additional information collected by the portal server and transmitting the authentication number to the Internet TV for storage if the authentication number is not already available; and

(c) transmitting information related to the message requesting authentication for use of information from the portal server to the Internet TV.

3. The method of claim 2, further comprising:

determining if the Internet TV is in a default state;

requesting the portal server to search for an authentication number corresponding to the Internet TV when the Internet TV is in a default state;

inputting user information requested by the portal server; and

receiving the requested authentication number and storing the received authentication number in a memory device.

4. The method of claim 2, further comprising:

if the authentication number is not available, requesting the portal server to provide a new authentication number with respect to the use of information; and

receiving a new authentication number from the portal server and storing the authentication number in a memory device.

5. The method of claim 2, wherein step (c) comprises:

(c1) examining the authentication number; and

(c2) receiving information from the portal server when it is determined from the examination of the authentication number that the authentication number is a normal authentication number.

6. The method of claim 5, further comprising:

providing user information requested by the portal server when it is determined from the examination of the authentication number that the authentication number is not a normal authentication number; and

receiving an authentication number transmitted from the portal server and storing the received authentication number in a memory device.

7. A method for accessing the Internet using an Internet TV, comprising:

(a) requesting a portal server to obtain an authentication number when the portal server receives an access request message from an Internet TV with respect to the use of information;

(b) transmitting a new authentication number from the portal server to the Internet TV if the authentication number is not provided by the Internet TV, wherein the new authentication number is established based on additional information collected by the portal server after the portal server receives the access request message if the authentication number is not provided by the Internet TV; and

(c) providing information related to the access request message with respect to the use of information to the Internet TV in response to the received access request message.

8. The method of claim 7, wherein the portal server remains in a stand-by state waiting for an access request message.

9. The method of claim 7, further comprising:

requesting the Internet TV to provide user information when the received access request message requests the portal server to search for an authentication number; and

determining whether a user is registered in a database when the user information is

received and transmitting an authentication number if the user is registered.

10. The method of claim 9, comprising:

requesting the Internet TV to provide user information when it is determined that a user is not registered in the database; and

assigning a new authentication number to the Internet TV when the user information is received and transmitting the assigned authentication number to the Internet TV.

11. The method of claim 7, further comprising:

checking for an error in the authentication number when the received access request message includes an authentication number;

determining whether the user is registered in a database when an error is not detected in the authentication number; and

providing information to the Internet TV according to whether a user fee is paid when it is determined that the user is registered in the database.

12. The method of claim 10, wherein the error is checked using a check sum method..

13. The method of claim 10, further comprising:

transmitting an error message when an error is detected in the authentication

number;

requesting the Internet TV to provide user information and determining whether the user is registered in the database; and

transmitting a corresponding authentication number when it is determined that the user is registered in the database.

14. The method of claim 10, further comprising registering the user in the database and providing information to the Internet TV when the user information is received.

15. The method of claim 10, further comprising:

determining whether a user fee is paid; and

transmitting a message to the Internet TV informing that the user fee is not paid if it is determined that the user fee is not paid.

16. The method of claim 7, further comprising:

requesting the Internet TV to provide the user information when the received access request message requests the portal server to provide a new authentication number; and

registering the user, assigning a new authentication number to the Internet TV, and transmitting the new authentication number when the user information is received.

18. The method of claim 1, wherein checking a validity of the transmitted authentication number comprises:

checking for an error in the authentication number; and

accessing user information in a database if an error is not detected in the authentication number; and

providing information to the Internet TV regarding user fees if the user information indicates that a user is registered.

19. The method of claim 18, further comprising:

transmitting an error message when an error is detected in the authentication number;

requesting user information from the Internet TV and determining whether the user is registered in the database; and

transmitting a corrected authentication number if the user is registered in the database.

20. The method of claim 1, further comprising determining if the Internet TV is in a default state.

21. The method of claim 1, further comprising storing the new authentication number in a memory device of the Internet TV.

22. The method of claim 4, further comprising registering a user in accordance with a user registration form requested by the portal server.

23. The method of claim 7, wherein the authentication number is accessed from a memory device of the Internet TV if the authentication number is provided by the Internet TV.

24. The method of claim 3, further comprising accessing the stored authentication number to gain access to the Internet during a later session.

EVIDENCE APPENDIX

Express Mail mailing label no. EL212282865US
Date of Deposit: March 2, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, BOX PROVISIONAL APPLICATION, Washington, D. C. 20231.

By: Vanessa Knowles

Attorney Docket No. TIVO0042PR

IN THE U.S. PATENT AND TRADEMARK OFFICE
Provisional Application Cover Sheet

Assistant Commissioner for Patents
BOX PROVISIONAL APPLICATION
Washington, D.C. 20231

Sir:

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(b)(2).

INVENTOR(s)/APPLICANT(s)

Last Name	First Name	Middle Initial	Residence (City and Either State or Foreign Country
Barton	James	M.	Los Gatos, California
Platt	David		Mountain View, California
Goodman	Andrew		Menlo Park, California
Zenchelsky	Daniel		Los Gatos, California

Additional Inventors are being named on separately numbered sheets attached hereto.

Title of the Invention

ENCRYPTION SYSTEM

Correspondence Address

GLENN PATENT GROUP
3475 EDISON WAY, STE. L
MENLO PARK, CA 94025

Telephone No. (650) 474-8400

Enclosed Application Parts *(check all that apply)*

(X) Specification and Drawing(s) *Number of Pages* 13

(X) Small Entity Statement - Business

( ) Other (specify)

Filing Fee and Method of Payment

__X__ $75.00 for Small Entity

_____ $150 for Large Entity

The Commissioner is authorized to charge the filing fee of $150 and any additional fees or credit any overpayment to Deposit Account No. 07-1445 (Order No. TIVO0042PR). A copy is enclosed for this purpose.

Respectfully Submitted,

MICHAEL A. GLENN
Reg. No. 30,176

Provisional Patent Application

Authors: Daniel Zenchelsky, Andy Goodman, David Platt

Background

MPEG is an industry standard for compressing, multiplexing, and transmitting digital video and audio. An MPEG stream is composed of a sequence of data bytes. These bytes can be logically grouped together to form a single element within an MPEG stream. For example, a single element within an MPEG stream might represent a single frame of video within a movie.

The MPEG standard defines byte sequences that indicate the start of an element within an MPEG stream. These byte sequences are referred to as □start codes.□

Some examples of MPEG start codes include: Video Packetized Elementary Stream Header, Video Group Of Pictures Header, Video I Frame Header, Video P Frame Header, Video B Frame Header, Video Slice Header, Audio Packetized Elementary Stream Header.

It is often useful or necessary to build an □Event Table□ that indicates the location of start codes within an MPEG stream. This table is composed of a list of offsets into the MPEG stream. The offsets listed in the table correspond to locations in the MPEG stream that contain start codes.

The Event Table may contain additional information as well. For example, it is often useful to describe what type of start code is located at each offset.

Using the Event Table allows a playback device to quickly locate a particular element within an MPEG stream. For example, one method of quickly scanning through video (□fast forward□) is to play only a subset of the video frames contained within the stream. The Event Table can be used to quickly locate those frames that need to be displayed.

One application where it is useful to build such a table is on a device designed to receive, store, and playback MPEG stream transmissions.

MPEG streams are often encrypted before transmission to prevent unauthorized use. It is often desirable to store the MPEG stream in it□s encrypted form prior to use, in order to prevent unauthorized use.

Typically, the stream is not decrypted until the rights to use the stream are purchased. The Event Table can not be built until the MPEG stream is decrypted. Building the Event Table can be a time consuming process. This can impose a significant time delay between the time that the rights to use the stream are purchased and the time that the Event Table is created and available for use.

Invention

1. When transmitting an MPEG stream using a broadcast or other transmission medium, transmit the Event Table along with the associated MPEG stream. This allows the receiver to have access to the Event Table without decrypting the MPEG stream.

2. Encrypt the Event Table itself prior to transmission, to protect it from unauthorized use.

Provisional Patent Application

Authors: Daniel Zenchelsky, Andy Goodman, David Platt

Background

Audio, video, and/or data can be broadcast as a digital transport stream. The headend is the system responsible for creating the transport stream. A receiver is a device that receives and displays (or uses) the transport stream.

The headend can encrypt the transport stream to protect from unauthorized viewing (or use) of the data stream. In that case, the receiver is capable of decrypting the transport stream prior to viewing (or using) it.

The encryption algorithm used to encrypt the transport stream is controlled by an encryption key. The key is necessary to decrypt the transport stream. The key can be changed on a regular basis to increase security. By changing it on a regular basis, there can be multiple keys required to decrypt the transport stream. The keys can then be encrypted and broadcast within the transport stream.

On a receiver, the transport reception module (TRM) is responsible for receiving the transport stream from the transmission medium.

On a receiver, the Conditional Access Module (CAM) is responsible for deciding whether or not to decrypt the stream, based on the services that the user has purchased. If the CAM allows the user to view/use the transport stream, it decrypts the keys and provides them to the Transport Decryption Module (TDM) for use in decrypting the transport stream.

On a receiver, the TDM is responsible for decrypting the transport stream. The TDM uses the keys provided by the CAM to decrypt the transport stream.

On a receiver, the display module is responsible for displaying the decrypted transport stream to the user.

Problem

It is useful to be able to record the transport stream in its encrypted form. However, current conditional access systems are subject to key replay attacks.

Example

Both user A and user B record the transport stream that contains a particular audio/video stream (e.g. a movie). User A purchases the service and the CAM in his receiver provides the keys for use in decrypting the transport stream. User A records the keys that

are provided by the CAM, and sends them to user B. User B is then able to decrypt the stream that he also recorded, using the keys provided by User A. User B is then able to view the audio/video stream without purchasing it.

Solution Requirements

Provide multiple layers of protection. If one layer is circumvented, the others remain intact.

Layer 1 - Prevent the keys from being recorded from the CAM. This can be done by never exposing the unencrypted keys to the user or any user programmable processor within the system, or storing it within any user accessible memory within the system. Further, the communication path between the CAM and the TDM can be encrypted.

Layer 2 - Prevent the keys from being played back into the TDM. This can be done by ensuring that the TDM will not accept the actual key to the TDM, but instead requires a key that is transformed in such a way that it is unique to a particular receiver. Likewise, the CAM must be designed to provide such a transformed key.

One factor in the effectiveness of this layer is the difficulty in transforming a key received from one receiver□s CAM into the key required by a second receiver□s TDM. The more difficult this is, the better the protection.

Layer 3 — Prevent the user from decrypting the transport stream without using the TDM. This can be done by never exposing the transport stream to the user. The transport stream must be encrypted a second time before passing it through any user accessible memory, or through any user programmable processor within the system. This can be further enhanced by providing an encryption mechanism that produces a different encrypted stream on different receivers.

Implementation

The implementation is based on existing encryption technology, used in a new and unique way.

Headend has
Global Secret Key
Headend Private Key
Receiver□s Transport Public Key
Receiver□s CAM Public Key

TRM has
Transport Private Key
Headend Public Key

TDM has
Transport Private Key
Headend Public Key

CAM has
CAM Private Key
Headend Public Key
Global Secret Key
CAM Secret Key

CAM to TRM/TDM Pairing Procedure

1. Headend generates a random secret : S
2. Headend cryptographically signs S using Headend Public Key : HPK(S)
3. Headend encrypts S,HPK(S) using Transport Public Key : TPK(S,HPK(S))
4. Headend encrypts S,HPK(S) using CAM Public Key : CPK(S,HPK(S))
5. Headend transmits TPK(S,HPK(S)) and CPK(S,HPK(S)) to TRM
6. TRM decrypts TPK(S,HPK(S)) using Transport Private Key : S,HPK(S)
7. TRM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
8. TRM stores shared secret, S, for future use
9. TRM passes TPK(S,HPK(S) to TDM
10. TDM decrypts TPK(S,HPK(S)) using Transport Private Key : S,HPK(S)
11. TDM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
12. TDM stores shared secret, S, for future use
13. TRM passes CPK(S,HPK(S)) to CAM
14. CAM decrypts CPK(S,HPK(S)) using CAM Private Key : S,HPK(S)
15. CAM verifies signature of HPK(S) using Headend Public Key. If signature is invalid, the processing stops here.
16. CAM stores shared secret, S, for future use

Transport Stream Recording Procedure

1. Headend generates an encryption key : K
2. Headend encrypts key using Global Secret Key : GSK(K)
3. Headend transmits GSK(K) to TRM
4. Headend encrypts transport stream using K : K(TS)
5. TRM sends GSK(K) to CAM
6. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key : LK= CSK(GSK(K))
7. CAM encrypts LK using shared secret, S : S(LK)
8. CAM sends S(LK) to TRM
9. TRM decrypts S(LK) using shared secret, S : LK
10. Headend transmits K(TS) to TRM
11. TRM further encrypts K(TS) using LK : LK(K(TS))
12. TRM stores GSK(K) and LK(K(TS)) on a storage medium

Transport Stream Playback Procedure

1. TDM retrieves GSK(K) and LK(K(TS)) from storage medium
2. TDM sends GSK(K) to CAM
3. CAM generates Local Key by encrypting GSK(K) using CAM Secret Key : LK= CSK(GSK(K))
4. CAM decrypts GSK(K) using GSK : K
5. CAM encrypts K,LK using shared secret, S : S(K,LK)
6. CAM sends S(K,LK) to Transport
7. TDM decrypts S(K,LK) using shared secret, S : K,LK
8. TDM decrypts LK(K(TS)) using LK : K(TS)
9. TDM decrypts K(TS) using K : TS
10. TDM sends Transport Stream, TS, to display module

Downloading Movies to Lots of People

James Barton

Elements:

- A population of TiVo Receivers
- A network supporting multi-cast packet transport
- A central scheduling system
- A server containing content of interest

Scenario:

- TiVo service produces program guide info describing programs stored on the video server and distributes it to TiVo receivers

- Viewer chooses a program for "recording". Instead of scheduling a recording, receiver sends request for the program to the TiVo service.

- TiVo service collects all requests and forwards them to a scheduling system. For most requested program, scheduling systems asks server to reliably multicast the program over the network to all receivers requesting it.

- When delivery is finished, the scheduler chooses another program to multicast. The choice can simply be to send the currently most requested program. This won't be good, as less requested programs may never be sent ("denial of service"). Thus, the scheduler will weight each program by the time since it was requested, with a limiting time perhaps a few days. If the limit is reached, that program is next to send. If several programs in that state, first-come, first sent. If the weighted desireablity of the program exceeds that of the most popular program, the weighted program is sent next instead. This guarantees that the program will eventually be sent in a timely manner.

- There is no requirement or need that this delivery occur in real time.

Permutations:

- Multiple programs may be delivered at once if sufficient resources are available. This is a simple extension to the above scheduling system.

- Multicast is not strictly required. In this case, the program

is sent separately to each receiver. In this case, resources will limit the number of parallel streams. Scheduling is based on a business model that might take into account such factors as: viewer pays a premimum for fast delivery, pays a discount for "whenever" delivery; content provider pays a premium for "fast" delivery, or gets a discount for "whenever" delivery.

- Movies may be encrypted for delivery.

-end-end-end-end-end-

TiVo Receiver to TiVo Receiver Interactions

J. M. Barton

1. Introduction

Currently, TiVo receivers communicate only with the TiVo Service Center, which provides program guide data, graphical resources (such as fonts, pictures, etc.), service information, and other forms of data that enable the receiver to operate independently of the service to satisfy viewer interests. This communication uses a secure distribution architecture to move data between the receivers and the service such that service data is protected as well as the viewer's privacy.

It would be highly desireable to have a mechanism for moving media and database elements between two TiVo receivers. For instance, a "portable" receiver might provide a smaller amount of disk storage in a battery-driven device. Before going on vacation, the viewer might transfer desireable media (and, invisibly, associated service data) to the portable receiver, and take the portable receiver along, such that the media might be used when desired.

There are other receiver interactions that are also highly interesting, but transfer only control information of some kind. For instance, it might be desireable to slave two recievers together, such that two media streams are played with precise synchonization.

"Synchronizing" two receivers, such that resources, software and media streams are transferred between the two to achieve identical operation are also of interest.

2. Transferring Media Streams

A TiVo stored media stream really consists of two pieces: the content itself, and a database object which gives descriptive information about the content.

There are many ways in which to connect two TiVo receivers. The simplest is to plug the output of the source into the input of the destination. While functional, this method fails to transfer information about the media stream, which is essential to viewer satisfaction in managing and using the media stream.

If a data transfer method is used, such as a network (e.g., IEEE 802.3) or a direct connection (e.g., IEEE 1394), then both the content and the descriptive information can be transferred, such that the integrity of the viewer experience is preserved.

Content owners are concerned about theft of content. A further refinement of this method is to encrypt the data transfer between the receivers. This can be done in a number of standard and custom ways. For instance, the Diffie-Hellman secure connection protocol might be used to encrypt the transfer using a one-time key.

If it were desireable to allow the transfer to only occur to certain specified receivers, the integrated security system might be used. The public key of each receiver must be known to the other. When the transfer is started, the receivers exchange signed, encrypted certificates based on the stored private key. If both receivers can decrypt and verify the signature of the other, a one-time session key is then used to encrypt the data during the transfer.

Key distribution in such a case might be handled through the TiVo Service. A viewer would contact the service, and request that two receivers he owns be authorized for data transfer between each other. The service center would send a authorization object containing each receiver's public key to the other receiver through whatever download mechanism is appropriate. The TiVo service could maintain a record of this operation for later auditing purposes, which would include identifying information for each receiver.

For instance, should the security system be defeated in the receiver and the public key of the other be exposed, it might be possible to modify other receivers such that they appear authorized to the source receiver. Each receiver might keep a record of transfers which is uploaded to the service center. Later, this information could be processed to look for copy protection violations, copies to unauthorized receivers, etc.

If the transfer is interrupted, the destination reciever marks the media stream as "partial" in the descriptive object, much as is done today. Later, the transfer might be restarted. Since the design of the database system guarantees the media stream can be uniquely identified on the target device, the partial stream is found, and the transfer begins from it's end, thus avoiding re-transfer of media that has already been stored. Once all the stream is stored, the descriptive object is updated to show a complete media stream.

3. Download Speed

There is no particular real-time requirement necessary when transferring digital data between the receivers. Thus, the transfer might take place at whatever speed is appropriate. For instance, it may be the case that the network between the receivers is slow, in which case the transfer

duration will be longer than the playback duration of the content.

Alternatively, the network may be fast, in which case multiple media streams might be transferred in much less time than taken for playback of one content item. As happens today, the viewer on the target system may start viewing the media stream as soon as the first portions are available, in parallel with the ongoing download of the stream.

4. Other Types of Transfers

There is no requirement that the source or destination system be a complete TiVo receiver. For instance, it may be the case that media streams are stored on a server in a cable head end. The same mechanism described here can be used to transfer the content and descriptive information reliably to the destination receiver.

Alternatively, the desintation system might be the same head-end server, and the TiVo receiver performs a transfer to it.

5. Pre-Encrypted Media Streams

Certain media distribution architectures, such as digital satellite systems, broadcast most content in an encrypted state. Using a local decryption facility based on a smart-card, the media is decrypted only if viewed, thus protecting the content from theft.

It is possible for the TiVo receiver to save these encrypted media streams to disk, and to initiate decryption upon playback. It is also possible to use the methods described here to transfer media between two TiVo receivers. In order to properly obey a particular set of content protection rules associated with the media stream (such as play once, expire after 1 day, etc.), the current TiVo receiver maintains with the database object describing the media stream the copy protection information associated with the stream (including whether the stream is stored encrypted).

It is possible to transfer these same rules to the destination TiVo receiver. For example, the receiver may have stored a movie from a distribution service that will not be decrypted until viewed. If the viewer wishes to have this media stream transferred, it is simply copied into the media region of the destination TiVo, and the descriptive object transferred as well. This means that all original information on the stream is faithfully duplicated to the destination receiver.

The smart-card might be pulled from the original receiver and installed in the second. When the content is viewed, the viewer is properly charged and all copy protection rules followed. The original media and descriptive information might, or might not, be removed.

For instance, in a "view-once" scheme, the originals are destroyed, whereas in a "charge-per-view" scheme, the would not.

6. Control Interactions

Using the same techniques as described earlier, a secure, or authenticated and secure, connection might be established between two or more receivers using a network, perhaps accessed using the internal modem.

This enables control interactions to take place. Some examples are:

- Synchronized playback. A viewer might control trick-play features on a particular media stream. Each key event is also passed to the slave receiver, which automatically performs the same action. For example, a presenter might give a live presentation using TiVo as a multimedia playback device. An audience at a remote location could watch the same presentation given in the same way at the same time. Alternatively, two viewers communicating through some other means, perhaps a phone, might interact, while one or the other controls the playback on both receivers of the same program. This could allow precise discussion of the program of interest. The means of communication might be a simple chat program overlayed on the display in which the participants type comments.

- Link passing. A viewer might indicate that a particular program be "linked" to the slave. This results in a message sent to the slave which causes it to schedule recording of that program. Alternately, the program might be "unlinked" as well. The message need contain only the program ID, assuming both receivers are in service.

- Sound or graphics effects. When the viewer takes an action, such as pressing a particular key sequence, the receiver might play a sound or present a graphic. It would pass that event to the slave receiver(s) which would reproduce that same sound or graphic. For instance, a child might add sounds to a program this way, which would be replicated for his friend on a remote receiver. Clearly, such communication would be multi-way.

7. Updates

It may be useful for receivers to be able to transfer other types of data as well. For example, consider a large "home" receiver and a smaller "portable" receiver. Interesting data, such as software, graphical elements, program guide data, etc., might be transferred between two receivers as well, using the well-understood methods described in the database patent and the security provisions described earlier.

For instance, the portable receiver might be "updated" by the home

receiver every time the two are connected. This update might include transferring and installing a software update as well. The portable receiver would transfer any operational information to be sent to the TiVo service to the home receiver, which would later transfer it to the TiVo service.

One can also contemplate "automatic" operation. In such a case, when two receivers are connected, a set of pre-configured actions takes place, such as updating program guide or software, and then media streams might be transferred as well. If the destination system is smaller, then not all media streams would fit. In this case, the viewer might explictly choose which streams to transfer. A more interesting case occurs if preference information is used to choose a subset of the available media of most interest to the viewer and transfer only those streams. Another case might be where media streams are transferred going from newest to oldest, stopping when no more will fit, or oldest to newest, which is less interesting. Another criteria might be whether the program was explicitly picked or chosen based on viewer preferences. Any program information stored in the descriptive object for the content might be used in the selection criteria, such as length, actors, rating, etc.

-end-end-end-end-end-

PTO/SB/10 (1-00)
Approved for use through 09/30/2000. OMB 0651-0031
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c))—SMALL BUSINESS CONCERN	Docket Number (Optional) TIVC0042

Patton et al.

Applicant, Patentee, or Identifier:
Application or Patent No.:
Filed or Issued: Herewith
Title: Encryption System

I hereby state that I am
- [X] the owner of the small business concern identified below
- [ ] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN: TiVo Inc.

ADDRESS OF SMALL BUSINESS CONCERN: 894 Ross Drive, Sunnyvale, CA 94089

I hereby state that the above identified small business concern qualifies as a small business concern as defined in 13 CFR Part 121 for purposes of paying reduced fees to the United States Patent and Trademark Office. Questions related to size standards for a small business concern may be directed to: Small Business Administration, Size Standards Staff, 409 Third Street, SW, Washington, DC 20416.

I hereby state that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention described in:

- [X] the specification filed herewith with title as listed above.
- [ ] the application identified above.
- [ ] the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention must file separate statements as to their status as small entities, and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization having any rights in the invention is listed below:
- [ ] no such person, concern, or organization exists.
- [X] each such person, concern, or organization is listed below.

Separate statements are required from each named person, concern or organization having rights to the invention stating their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

NAME OF PERSON SIGNING: James M. Barton

TITLE OF PERSON IF OTHER THAN OWNER: Sr. Vice President

ADDRESS OF PERSON SIGNING: 894 Ross Drive, Sunnyvale, CA 94089

SIGNATURE: [signature] DATE: Mar. 1, 2000